In re Patent Application of
LIARDET ET AL.
Serial No. **09/506,158**
Filed: **FEBRUARY 17, 2000**

REMARKS

The Examiner is thanked for the thorough examination of the present application. Independent Claims 11, 17, 25, and 30 have been amended to more clearly define the subject matter thereof over the prior art. Claims 13, 18-19, 21-22, 27-28, and 32-33 have been amended for consistency therewith, and Claims 26 and 31 have been canceled. Support for the amendments may be found on pages 12-13 of the originally filed specification and in FIG. 5, for example. No new matter is being added.

In view of the amendments and the supporting arguments presented in detail below, it is submitted that all of the claims are patentable.

I. The Claimed Invention

The present invention is directed to and electronic circuit for a cryptography coprocessor. As recited in amended independent Claim 17, for example, the electronic circuit includes a plurality of input/output registers having a scrambling register for receiving digital key data. More particularly, the digital data key includes a digital key and a plurality of scrambling bits intermixed with the digital key. The electronic circuit further includes an input register for receiving message data to be processed by the encryption or decryption operation, and a key register for receiving the digital key data for use in the encryption or decryption operation. A multiplexer transfers data between the plurality of input/output registers and the input register and the key

register. Moreover, a processor is connected to the scrambling register, the input register, and the key register and performs the encryption or decryption operation on the message data in the input register based upon the digital key data and the scrambling bits. The electronic circuit further includes a controller for controlling the plurality of input/output registers, the multiplexer and the processor, and an output register to transmit the result of the encryption or decryption operation to the plurality of input/output registers through the multiplexer.

The intermixed scrambling bits advantageously secure the loading of the digital key into the input/output registers. Yet, by separately storing the scrambling bits in the scrambling register, the processor may readily determine the digital key from the contents of the key register and the scrambling register, as discussed on pages 12 and 13 of the originally filed specification, for example. Independent Claim 11 is directed to a related electronic circuit, and independent Claims 25 and 30 are directed to related methods. Each of these claims has been amended similarly to Claim 17 to recite that the scrambling bits are intermixed with the digital key.

II. The Claims Are Patentable

The Examiner rejected independent Claims 11, 17, 25, and 30 based upon the prior art illustrated in FIG. 3 of the application and U.S. Patent No. 6,144,744 to Smith, Sr. et al. (hereafter "Smith"). While the Examiner acknowledges that the prior art shown in FIG. 3 of the present application fails to

In re Patent Application of
LIARDET ET AL.
Serial No. **09/506,158**
Filed: **FEBRUARY 17, 2000**

teach or fairly suggest using scrambling bits to secure a digital key, the Examiner contends that Smith provides this noted deficiency.

Smith discloses a method and apparatus for securely transferring objects (i.e., master keys) between different cryptographic processing modules. The master key transfer is accomplished using the Dieffie-Hellman key exchange protocol which allows a module to create a transport key for encrypting items to be transferred to a receiving module. Thus, the method of Smith allows the two modules to build a transport key to securely transfer a master key encrypted with the transport key.

In particular, the Examiner notes a transport key register **1620** in FIG. 16 of Smith, and he contends that this register is a scrambling register for storing scrambling bits as recited in the above-noted independent claims. Yet, Smith notes at col. 15, lines 40-45 and col. 17, lines 50 through col. 18, line 30 that the transport key stored in the register **1620** is merely a secret key used to encrypt an object protection key to be transferred between the modules. The transport key is not transferred with the encrypted object protection key between the modules. As such, the transport key is neither included as part of any digital key data to be transmitted, nor is it intermixed with the object protection key, as recited in each of the above independent claims. Thus, the selective combination of references proposed by the Examiner fails to teach or fairly suggest all of the elements recited in the above-noted independent claims.

Accordingly, it is submitted that independent Claims

In re Patent Application of
LIARDET ET AL.
Serial No. **09/506,158**
Filed: **FEBRUARY 17, 2000**

11, 17, 25, and 30 are patentable over the prior art. Their respective dependent claims, which recite yet further distinguishing features, are also patentable over the prior art and require no further discussion herein.

CONCLUSIONS

In view of the foregoing, it is submitted that all of the claims are patentable. Accordingly, a Notice of Allowance is respectfully requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,

JOHN F. WOODSON, II
Reg. No. 45,236
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
Telephone: 407/841-2330
Fax: 407/841-2343
Attorney for Applicants